IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOHNNY FLORES, ARIEL GOMEZ and DERRICK LEWIS, for themselves and others similarly situated, Plaintiffs, v. MOTOROLA SOLUTIONS, INC., and VIGILANT SOLUTIONS, LLC, Defendants.	)	Case No. 1:20–cv–01128 Judge Charles R. Norgle, Sr.

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Dated: July 15, 2020

Respectfully submitted,

/s/ Scott R. Drury
SCOTT R. DRURY

Arthur Loevy
Michael Kanovitz
Jon Loevy
Scott R. Drury
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
arthur@loevy.com
mike@loevy.com
jon@loevy.com
drury@loevy.com

INTRODUCTION

For good reason, the facial recognition business, and biometric data analysis more generally, is a highly regulated industry. These technologies present great risks to the affected individuals, including identity theft, surveillance, stalking and more. In Illinois, the Biometric Information Privacy Act ("BIPA") ensures that private companies cannot take a person's biometric information without consent and requires that the companies employ a host of safeguards to protect the individuals about whom they maintain this powerful personal information.

BIPA regulates the facial recognition business of Defendants Motorola Solutions, Inc. ("Motorola") and Vigilant Solutions, LLC ("Vigilant"), but Defendants are not complying with its safeguards. In fact, they are able to make a very nice profit primarily because they took the raw materials for their business—the biometric data—from millions of people without their consent. Unlike responsible companies that ask each individual before taking his or her biometric data as the law requires, Defendants just grabbed the data by extracting it from online photos without consent and without even revealing that they had done so. This mechanized fishing of biometric information from the internet allowed Defendants to create a massive biometric database far cheaper and far faster than their competition who comply with the law, but it was illegal. The very core of Defendants' business model relies on doing exactly what the law says that a private company cannot.

In their motion to dismiss, Defendants try to make their business model fit within the strictures of BIPA, but it is a square peg in a round hole. In each argument, Defendants are either stretching with interpretations that the statute will not bear, interpreting Plaintiff's First Amended Complaint in ways that violate the standard on a motion to dismiss, or both. Accordingly, the arguments all fail and the must be denied. Plaintiffs address each argument below.

FACTUAL BACKGROUND

I. Biometrics

Every individual has unique, immutable features by which he or she can be identified using a set of standard quantitative measurements. Dkt. 6 ¶ 1. Much like a fingerprint, each person also has a unique facial geometry composed of, among other measures, distances between key facial landmarks and ratios between those distances. *Id.* Fingerprints and facial geometric measurements are two forms of "biometric data." *Id.*

II. Defendants' Unlawful Biometric Database

Defendant Vigilant is a corporation that, as of January 2019, became wholly owned by Defendant Motorola. Dkt. 6 ¶¶ 19-20. Defendants are private entities that sell facial recognition products to government agencies and private companies throughout the U.S. *Id.* ¶¶ 29, 36. The facial recognition technology is based on "biometric algorithms of facial landmarks." *Id.* ¶ 37.

Beginning no later than 2014, Defendant Vigilant, with Defendant Motorola later joining, began obtaining "mugshot" photos from the internet, including those posted by the Illinois Department of Corrections ("IDOC"). *Id.* ¶¶ 4, 31, 41. After obtaining the mugshots, Defendants collected and captured facial biometrics of each person depicted in each mugshot and created a biometric database (the "Biometric Database"). *Id.* ¶¶ 4-5. The Biometric Database includes over 18 million mugshots and at least tens of thousands of Illinois residents. *Id.* ¶¶ 4, 40. Defendants included individuals in the Biometric Database based on the mere fact of an arrest. *Id.* ¶ 9.

Defendants sold access to, traded and otherwise profited from the Biometric Database by selling it to law enforcement agencies and others to use as a "facial search engine" to match "probe images" to the people in the database. *Id.* ¶¶ 8, 31-33, 36-40. Through use of the Biometric Database, a user could learn identifying information about the person in the probe image. *Id.* ¶¶ 8,

31-33, 39. By providing others with access to the Biometric Database, Defendants disclosed, redisclosed and otherwise disseminated the biometric data of the persons depicted in the mugshots. *Id.* ¶ 33. Defendants did not notify the persons in the mugshots of the fact that Defendants were collecting the persons' biometric data, nor did they obtain consent to do so. *Id.* ¶ 34.

III. Plaintiffs

At relevant times, Plaintiffs Derek Lewis, Johnny Flores and Ariel Gomez were Illinois residents incarcerated within the IDOC on charges for which they were innocent. *Id.* ¶¶ 14-16. In connection therewith, the IDOC took and posted on the internet each Plaintiff's mugshot. *Id.* On information and belief, Defendants obtained each Plaintiff's mugshot from the internet and collected, captured, sold, traded, profited from, disclosed, redisclosed and otherwise disseminated each Plaintiff's biometric data. *Id.* ¶¶ 14-16, 31-33, 41-48. Defendants engaged in this alleged conduct without: (a) providing notice to Plaintiffs; (b) obtaining their consent; or (c) utilizing a reasonable standard of care to protect the biometric data from disclosure. *Id.* ¶¶ 44-45.

IV. The Complaint

On February 14, 2020, Plaintiffs filed a class action complaint against Defendants alleging multiple violations of BIPA and unjust enrichment and seeking injunctive relief. *See* Dkt. 1. Plaintiffs subsequently amended the complaint (the "Amended Complaint"). Dkt. 6. In the Amended Complaint, Plaintiffs seek to represent a class of Illinois residents whose faces appeared in the Biometric Database from February 14, 2015 to the present. *Id.* ¶ 55.

ARGUMENT

I. Legal Standards.

A. Fed. R. Civ. P. 12(b)(6).

At the Rule 12(b)(6) stage, "the well-pleaded factual allegations . . . are taken as true and considered in the light most favorable to plaintiffs . . . ." *Reed v. Palmer*, 906 F.3d 540, 549 (7th Cir. 2018). "[W]hen considering a motion to dismiss under Rule 12(b)(6), a court must draw all reasonable inferences in favor of the non-moving party." *Vesuvius USA Corp. v. Am. Commercial Lines LLC*, 910 F.3d 331, 334-35 (7th Cir. 2018).

B. BIPA

Illinois strictly regulates the collection and use of two kinds of biometric data: "biometric identifiers" and "biometric information." *See* 740 ILCS § 14/1, *et seq.* Under Illinois law, biometric identifiers are defined to include, *inter alia*, a "scan of . . . face geometry." 740 ILCS § 14/10. Biometric information, in turn, is "any information . . . based on an individual's biometric identifier used to identify an individual." *Id.* BIPA prohibits private entities such as Defendants from, among other things: (a) collecting, capturing or otherwise obtaining an individual's biometric data without providing written notice and obtaining a written release; (b) selling, leasing, trading or otherwise profiting from an individual's biometric data; and (c) disclosing, redisclosing or otherwise disseminating an individual's biometric data in the absence of circumstances specifically set forth in the statute. *See* 740 ILCS § 14/15.

II. Defendants Are Not Exempted from BIPA.

Defendants seek an exemption for their entire business model under BIPA § 25(e), contending that all of their conduct, no matter when it was undertaken or why, is exempt under the statute's carve-out for government-contractor activities. Dkt. 25 at 6. This contention flies in the

face of the statutory text. Section 25(e) provides that "[n]othing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government ***when working for that State agency or local unit of government.***" 740 ILCS § 14/25(e) (emphasis added). According to Defendants, the mere fact that they sold their product to police departments exempts all of their conduct from BIPA (Dkt. 25 at 6), even though they: (a) created the Biometric Database without being instructed to do so by the government; (b) sell their product to non-government clients; and (c) control critical business decisions, such as whether to sell their product at all, and at what price. *See* Dkt. 6 ¶¶ 5, 8, 31-33. The Amended Complaint's allegations and BIPA's plain language do not support Defendants' strained interpretation.

Nowhere in the Amended Complaint do Plaintiffs allege that Defendants collected, captured, sold, traded, profited from, disclosed, redisclosed or otherwise disseminated Plaintiffs' and Class Members' biometric data pursuant to a government contract or "when working for [a] State agency or local unit of government." Rather, Plaintiffs allege that Defendants surreptitiously collected and captured Plaintiffs' and Class Members' biometric data, used it to create the Biometric Database, and then sold the database on the open market – to government entities and others. Dkt. 6 ¶¶ 4-5, 8, 31-33.

Similarly, nowhere in BIPA does it provide the broad exemption Defendants seek. Defendants contend that the Illinois legislature "recognized that, to prevent BIPA from being applied indirectly to regulate government activities, it would also be necessary to exempt from the reach of the statute private entities that provide products and services to the government." Dkt. 25 at 6. But BIPA does not go nearly that far. While it is true that § 25(e) exempts private companies from liability for actions undertaken while acting under the direction of the government, it does not exempt all conduct of "private entities that provide products and services to the government,"

as Defendants contend. To accept Defendants' interpretation would read out of § 25(e) its express language that it only applies to entities "when working for" the government – violating the maxim that "a court should not construe a statute in a way that makes words or phrases meaningless, redundant, or superfluous." *United States v. Franz*, 886 F.2d 973, 978 (7th Cir. 1989) (internal citation and quotation marks omitted).

While not alleged in the Amended Complaint, Defendants contend that they performed some work for the government. *See* Dkt. 25 at 6. The contention does not change the above-described conclusion, but merely indicates that Defendants may not be liable for a narrow set of conduct. Notably, Plaintiffs do not seek to recover for the work described – *i.e.*, assisting with identifying persons in probe images – as the defined class only includes people appearing in the Biometric Database, not probe images. Thus, whatever work Defendants may perform for government (or other) clients when those clients provide Defendants with probe images, prior to performing that work, Defendants have already violated BIPA in multiple ways.

Finally, apart from any work Defendants may have performed for government entities, as discussed above, the Amended Complaint also alleges that Defendants sold their product to private businesses and other third parties. *See* Dkt. 6 ¶¶ 5, 8, 36. Under no reading of § 25(e) would Defendants' business dealings with non-governmental entities enjoy blanket exemption from the statute simply because Defendants also sell their products or services to government customers.

III. The Amended Complaint Alleges a Violation of BIPA § 15(b).

Defendants argue that the absence of a direct relationship between them and the people in their database precludes any possibility of Defendants having violated BIPA § 15(b). Dkt. 25 at 7-9. They further contend that § 15(b) does not apply to the collection or capture of biometric data from public photos. *Id.* at 9. Defendants are wrong on both fronts. By choosing a business model

that surreptitiously collects biometric data without the knowledge or consent of individuals who never sought out any relationship with the entity doing the collecting, Defendants made their violations of the statute more serious, not less. And Defendants' supposed "public photo" exemption has no support in the statutory text or in the relevant case law.

A. Section 15(b) Does Not Contain a Direct Relationship Requirement.

Section 15(b) sets forth a notice-and-consent requirement that applies categorically to the collection and capture of all persons' biometric data and contains no exceptions or qualifications: "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain ***a person's*** or a customer's biometric identifier or biometric information" without providing notice or obtaining consent. 740 ILCS § 14/15(b) (emphasis added). It is a well-settled canon of statutory construction that a court should interpret statute so as to give meaning to every word set forth therein. *See, e.g.*, *Seitz v. City of Elgin*, 719 F.3d 654, 657 (7th Cir. 2013). Here, the legislature's use of both "person" and "customer" in § 15(b) demonstrates that it intended those terms to have separate meanings. Whereas "customer" indicates the "direct relationship" advocated by Defendants, "person" necessarily requires a different interpretation. Where a word or phrase has a common meaning, a court should use that definition. *See, e.g., Sandifer v. U.S. Steel Corp*., 571 U.S. 220, 227 (2014).

The broad application of § 15(b) discussed above accords with the Illinois Supreme Court's interpretation of BIPA. *See Rosenbach v. Six Flags Entm't Corp*., 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court has emphasized that BIPA codified a privacy right available to all individuals. *See id.* at 1206 ("[O]ur General Assembly has codified that ***individuals*** possess a right to privacy in and control over their biometric identifiers and biometric information."); *id.* (BIPA violation constitutes an "invasion, impairment, or denial of the statutory rights of any

person or customer"); *id.* ("***individuals*** and customers" have the right to control their biometric information") (emphases added). Moreover, the Illinois Supreme Court has held that BIPA serves a "preventative and deterrent purpose[]," namely, to give all individuals control over the fate of their biometric data before "substantial and irreversible harm . . . result[s] if biometric identifiers and information are not properly safeguarded . . . ." *Id.* at 1207.

Notably, Defendants' unsupported interpretation of § 15(b) runs directly counter to the prophylactic nature of BIPA as described by the Illinois Supreme Court. If BIPA failed to protect individuals from third-party companies that collect and capture biometric data, those companies could inflict "substantial and irreversible harm" without first allowing the individual to exercise control over the fate of his or her own data. As the Illinois Supreme Court refused to do, this Court should decline Defendants' invitation to "read into the statute conditions or limitations the legislature did not express, and interpret the law in a way that is inconsistent with the objectives and purposes the legislature sought to achieve." *Id.*

Beyond the Illinois Supreme Court's broad interpretation of BIPA, several courts in this District – including this Court – have applied BIPA to defendants that collected biometric data from individuals with whom they had no existing relationship. In *Norberg v. Shutterfly, Inc.,* 152 F. Supp. 3d 1103 (N.D. Ill. 2015), this Court held that the plaintiff had alleged a Section 15 violation despite having never interacted with the defendant: "Plaintiff alleges that Defendants are using his personal face pattern to recognize and identify Plaintiff in photographs posted to Websites. Plaintiff avers that ***he is not now nor has he ever been a user of Websites*** . . ." *Id.* at 1106 (emphasis added). Since *Norberg*, other courts in this District have held that § 15(b) applies to claims against defendants that have no prior relationship or interaction with the plaintiffs. In *Rivera v. Google Inc.,* 238 F.Supp.3d 1088 (N.D. Ill. 2017), the court denied Google's motion to

dismiss a plaintiff's claims where the plaintiff alleged that: (a) Google extracted her biometric data from photos other people had taken of her on their Android devices; and (b) she did not have a Google Photos account. *Id.* at 1090-91; *see also Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017) (finding plausible BIPA claims against Shutterfly where the plaintiff "[did] not use Shutterfly and never consented to Shutterfly's extraction and storage of data representing his face geometry").

While Defendants correctly note that § 15(b) requires a written exchange between the entity collecting the biometric data and the individual (Dkt. 25 at 7), nothing about that requirement allows the collecting entity to forego the written exchange merely because of the lack of a direct relationship. *See* 740 ILCS § 14/15(b). Defendants seek to have the Court read into the statute an "inconvenience" exception that simply is not there; § 15(b) is clear on its face, and the fact that Defendants' chosen business model becomes burdensome or costly if they comply with the law as written is of no consequence. The Court should reject Defendants' unsupported interpretation.

Relatedly, Defendants' contention that there "would not be any feasible way" to provide notice to or obtain consent from the affected individuals (Dkt. 25 at 8) suffers from the same fundamental flaw. Defendants are not at liberty to choose an illegal business method. Moreover, this argument is a non-starter at this stage of the proceedings and relies on inferences drawn in Defendants' favor. The Amended Complaint alleges that Defendants collected the biometric data of at least tens of thousands of Illinois residents from websites that listed the names of such individuals, among other identifying information. Dkt. 6 ¶¶ 31-32. It is reasonable to infer that Defendants could have contacted them and sought consent if they had chosen to do so.

Defendants' citation to *dicta* from a single Illinois trial court decision, *Bernal v ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *1 n.9 (Ill. Cir. Ct. Aug. 23, 2019), does not support

the unconstrained statutory exception they have invented. In *Bernal*, because an employee had already given his employer his biometric information and could have withheld consent at that stage, the court suggested in a footnote that the employee could not later seek to withhold that consent from a vendor that provided the biometric technology to the employer. *Id.* ("[T]here is little reason to believe that its applicability should extend beyond the point at which an individual has the right to withhold consent."). Here, there is no evidence that Plaintiffs and Class Members ever provided consent to — or had the opportunity to withhold consent from — any entity to scan their facial geometries. Moreover, the court in *Bernal* ultimately dismissed the plaintiff's § 15(b) claim not because of a lack of a "direct relationship," but rather because the "Plaintiff . . . failed to allege facts sufficient enough for the Court to properly assess Defendant's actual involvement" in the biometric data collection.[1] *Id.* There is no such problem here. The Amended Complaint makes clear that Defendants themselves are responsible for the collection of Plaintiffs' and Class Members' biometric data in violation of the statute. *See, e.g.*, Dkt. 6 ¶¶ 3-8, 31-33.

B. BIPA Contains No Public Records Exception.

Defendants make a red herring argument that BIPA does not apply to biometric data collected or captured from "booking photos [because they] have been made publicly available." Dkt. 25 at 9. According to Defendants, BIPA protects confidential and sensitive information and "[a]ny information that is publicly available by its very nature cannot be confidential . . . ." *Id.* The argument misses the mark, because the biometric data – which is what the statute protects – is not and has never been made public. Taking Defendants' argument to its logical conclusion, anyone who exposes his or her face in public would be waiving protections of the statute because Defendants could then use a camera to extract the person's biometric data in the same manner as

[1] Unlike here, the defendant in *Bernal*, a payment processer, was a "third party" separate from the individual whose biometric data was being collected and the private entity that was collecting it. *Id.* at *1.

with their booking photos. The argument also fails because there simply is no exception in the statute allowing a company to profit from biometric data that it gleans from images in public view.

Notably, BIPA has been applied to unauthorized biometric scans of photographs that individuals made public. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 2369 (9th Cir. 2019) (applying BIPA to Facebook's extraction of biometric data from any photograph in which a user appeared, with no distinction between public and non-public photographs). Defendants' claim to the contrary lacks merit. Dkt. 25 at 9. Defendants' contention that Plaintiffs and Class Members gave up their right to control their biometric data because a third-party posted their photos online also confuses the difference between the photos themselves and the biometric data that Defendants unlawfully extracted therefrom without notice or consent.[2] Simply put, a person whose photo becomes public has not consented to the extraction of his or her biometric data from that photo.

To accept Defendants' proposed interpretation of § 15(b) would create an exception that would swallow the rule. Under Defendants' interpretation, the biometric data of every Illinois resident whose photo, fingers or eyes appears online could freely be harvested by any third party who chooses to do so – *i.e.*, facial geometric scans, fingerprints, and retina scans would all be fair game.[3] Nothing in the statutory text nor in the Illinois Supreme Court's decision in *Rosenbach* hints at such a giant loophole. On the contrary, Defendants' interpretation is impossible to square with the Illinois Supreme Court's holding in *Rosenbach* that BIPA put a "preventative and

[2] In *Rivera*, the court aptly noted the distinction, finding that irrespective of the "medium" from which it is derived or the "way of taking measurements" used, a "set of measurements of a specified physical component (eye, fingers, voice, hand, face) used to identify a person" is a "biometric identifier" under BIPA. *Rivera*, 238 F.Supp. 3d at *1096.

[3] Fingerprints and retinal scans can be obtained from photographs, a fact the court in *Monroy* cited as support for its holding that the statute applied to biometric data collected from photographs. *See Monroy*, 2017 WL 4099846, at *4.

deterrent" framework in place to prevent the "substantial and irreversible harm" that can occur when biometric data is obtained without consent. 129 N.E. 3d at 1207.

Finally, Defendants' contention that application of § 15(b) to this case would be inconsistent with the BIPA's legislative purpose of "*encourag[ing]* the 'use of biometrics' while protecting the privacy rights of Illinois residents" (Dkt. 25 at 9 (emphasis in original)), lacks merit. BIPA contains no such findings, *see* 740 ILCS 14/5, but rather has the announced purpose of ensuring that citizens maintain control of their biometrics, *see* 740 ILCS § 14/5(g). Application of § 15(b), as discussed herein, is, thus, perfectly in line with BIPA's legislative intent.[4]

IV. The Amended Complaint Alleges a Violation BIPA § 15(c).

Contrary to Defendants' assertions (Dkt. 25 at 10-11), Defendants violated BIPA § 15(c) by selling, leasing, trading or otherwise profiting from Plaintiffs' and Class Members' biometric data. The Amended Complaint specifically alleges how Defendants profited from the biometric data by: (a) developing the Biometric Database (Dkt. 6 ¶ 38); (b) comparing customers' probe images to the database to find matches (*id.* ¶¶ 37, 39); and (c) offering access to the database for a fee to law enforcement agencies and others throughout the country (*id.* ¶ 8). *See also id.* ¶¶ 33, 42. Only by ignoring these allegations and the inferences therefrom can Defendants conclude that Plaintiffs fail to allege a § 15(c) violation. Indeed, Defendants' entire business model is premised on collecting and capturing biometric data and then profiting from that data when customers pay to search it.

Defendants' contention that they somehow do not sell biometric data (Dkt. 25 at 10-11) fails. BIPA regulates the collection, possession, and use of two different types of biometric data:

[4] If Defendants mean to convey that BIPA exempts the extraction of Biometric Identifiers from photographs in general, they are wrong. Every court to address this argument, including this Court, has rejected it. *Norberg*, 152 F. Supp. 3d at 1105-06; *Rivera,* 238 F.Supp.3d at 1092-1100; *Monroy,* 2017 WL 4099846, at *2-5; *In re Facebook Biometric Info. Privacy Litig.,* 185 F.Supp.3d 1155, 1171 (N.D. Cal. 2016).

"biometric identifiers" and "biometric information." *See* 740 ILCS § 14/10. By performing facial geometric scans and acquiring the resulting measurements, Defendants obtain "biometric identifiers." *See id.* As alleged, Defendants then use those biometric identifiers to develop "biometric information," which is defined as "***any*** information, regardless of how it is captured, converted, stored, or shared, ***based on an individual's biometric identifier used to identify an individual.***" *Id.* (emphasis added); *see* Dkt. 6 ¶ 32. When Defendants get paid to search a database containing biometric information on Plaintiffs and Class Members to find a potential match, they are doing precisely what the statute forbids: "profit[ing] from a person's . . . biometric identifier or biometric information."

Even if Defendants did not sell Plaintiffs' and Class Members biometric information, their conduct still violates § 15(c) because they grant access to Plaintiffs' and Class Members' biometric identifiers in exchange for a fee. Dkt. 6 ¶ 8. Defendants' customers pay for access to the entire Biometric Database so that their probe image can be searched against all the possible matches. *Id.* Defendants are able to offer those known identities through their collection of biometric identifiers and information.[5] *Id.*

Finally, Defendants' attempt to write § 15(c)'s "or otherwise profit from" language out of the statute (Dkt. 25 at 10-11) lacks merit. According to Defendants, the legislature's use of the phrase "or otherwise profit from" has no distinct meaning from the words "sell," "lease," or "trade." *Id.* However, this construction fails to give meaning to each word in the statute. *See supra*

[5] Accepting Defendants' view of the facts still results in a § 15(c) violation. Whether one calls the product Defendants offer a rental of Plaintiffs' biometric identifiers, a temporary license, or a lease, the precise form of the transaction is immaterial to the conclusion that Defendants "profit[ed] from" the biometric data. In exchange for consideration, customers can "access and use" the facial geometric measurements in the database. Dkt. 6 ¶ 8. Just as Microsoft might grant a license to (or "sell" or "lease") Microsoft Word software without giving up every detail of the source code, so too do Defendants grant their customers use of Plaintiffs' and Class Members' biometric identifiers.

at 7. If "otherwise profit from" were merely "meant to reinforce the prohibition on selling, leasing, or trading biometric data" (*see* Dkt. 25 at 11), the phrase would be superfluous. The purpose of the phrase was to reach all ways of profiting from biometric data, which Defendant clearly does.

V. The Amended Complaint Alleges a Violation of BIPA § 15(d).

As explained above, when Defendants' customers upload a probe image to the Biometric Database for identification, Defendants send the customers potential matches based on a comparison of the probe image's biometric identifiers with those of individuals already in the Biometric Database. Every time Defendants send out those matches, they disclose, redisclose and otherwise disseminate biometric information in violation of BIPA § 15(d). Biometric information is "***any*** information, ***regardless of how it is captured, converted, stored, or shared***, based on an individual's biometric identifier used to identify an individual." 740 ILCS § 14/10 (emphasis added). As alleged, the Biometric Database contains Plaintiffs' and Class Members' names and other identifying information (Dkt. 6 ¶ 32) – *i.e.*, their biometric information. It is reasonable to infer that Defendants disclose this biometric information to their customers in connection with matching a probe image to images in the Biometric Database, otherwise the database would be of little use.

Defendants contention that they somehow do not violate § 15(d) because they provide their results in the form of an image gallery (*see* Dkt. 25 at 17) lacks merit. Regardless of the format in which Defendants disclose, redisclose and otherwise disseminate Plaintiffs' and Class Members' biometric information, the fact remains that they do disclose the information – which violates § 15(d).

VI. The Amended Complaint Alleges a Violation of BIPA § 15(e)

By freely making Plaintiffs' and Class Members' highly sensitive biometric data available to countless paying customers, Defendants have committed a clear violation of BIPA § 15(e), which requires Defendants to: (a) "store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is ***the same as or more protective*** than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information"; and (b) "store, transmit, and protect from disclosure all biometric identifiers and information using the reasonable standard of care within the private entity's industry." 740 ILCS § 14/15(e) (emphasis added). Defendants cannot credibly contend that their disclosure of biometric data to anyone willing to pay a price conforms with the way in which they protect other confidential and sensitive information or industry standards.[6]

VII. Plaintiffs Have Pleaded a Plausible Claim for Unjust Enrichment

Defendants' unjust enrichment arguments and the authority they cite advance the proposition that an unjust enrichment claim requires some independent basis for liability. Dkt. 25 at 13-14. Contrary to Defendants' contention and as discussed throughout, Plaintiffs have alleged numerous BIPA violations. Accordingly, there exist no grounds for dismissing Plaintiffs' unjust enrichment claims at this stage.

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' motion to dismiss in its entirety. However, if the Court grants any portion of the motion, Plaintiffs request leave to replead.

[6] Based on the Seventh Circuit's recent ruling in *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020), Plaintiffs do not oppose Defendants' Rule 12(b)(1) motion to dismiss Plaintiffs § 15(a) claim.

CERTIFICATE OF SERVICE

I, Scott R. Drury, an attorney, hereby certify that, on July 15, 2020, I filed the foregoing document using the Court's CM/ECF system, which effected service on all counsel of record.

/s/ Scott R. Drury
One of Plaintiffs' Attorneys